

ПРОГРАММА-СИМУЛЯТОР ПАК «СИГУРД»

И. А. Кишеева, А. А. Пипкина

(Екатеринбург, УрФУ, makkuropip@gmail.com)

1. Цель

Целью проекта является создание программы-симулятора ручного режима работы ПАК «Сигурд», предназначенной для обучения студентов основам работы с данным комплексом, методикам проведения специальных исследований технических средств, для приобретения навыков последующей работы с реальным комплексом и его аналогами.

Программа-симулятор направлена на упрощение учебного процесса в части освоения студентами методов оценки защищенности информации от утечки по каналам ПЭМИН и обеспечивает закрепление на практике следующих знаний:

- общей методики поиска, верификации и измерения сигналов ПЭМИ в ручном режиме;
- анализа вида и параметров искомого сигнала в зависимости от исследуемого ОТСС и используемого тестового режима;
- определения частот, в окрестностях которых следует ожидать появления опасных сигналов;
- выбора измерительной антенны, подходящей для проведения измерений в конкретном диапазоне частот.

Поскольку в силу высокой стоимости ПАК каждый студент на лабораторной работе не может быть обеспечен возможностью индивидуальной работы с комплексом, получение базовых навыков работы с комплексом на виртуальном приборе является единственным выходом из данной ситуации. Так как поняв, какие сигналы нужно искать, как проводить поиск, верификацию и измерение сигналов, работая в программе-симуляторе, студент затем быстро освоит технику работы с реальным комплексом.

2. Методика проведения измерений ПЭМИ с помощью ПАК «Сигурд»

Порядок инструментального контроля ПЭМИН:

1) измерение уровней ПЭМИ и наводок информативных сигналов:

- а) электрической составляющей;
- б) магнитной составляющей;
- в) индуктивной составляющей наводок в симметричных и несимметричных линиях как гальванически связанных, так и не связанных с проверяемым устройством, но имеющих выход за границы КЗ;

- г) измерение реального затухания в опасных направлениях на границе КЗ;

- д) измерение параметров применяемых средств защиты;

2) измерение уровней шума на частотах опасного сигнала;

3) расчет выполнения нормы и оценка защищенности;

4) оформление протоколов по результатам проведенных проверок.

Согласно действующим нормативно-методическим документам при проведении специальных исследований требуется измерять информативные ПЭМИ. Такие излучения составляют лишь малую долю от всего спектра излучений технического средства. Все прочие излучения не должны фиксироваться при измерениях.

Для того чтобы выделить информационные ПЭМИ, на исследуемом техническом средстве предусматривают специальные тестовые режимы его работы.

Измерение собственных электромагнитных излучений технических средств включает в себя следующие операции:

1. Контролируемое устройство включается в тестовый режим.

2. На определенном расстоянии (обычно 1 м) от устройства поочередно устанавливаются антенны для измерения электрической и магнитной составляющих поля, излучаемого устройством.

3. Электрический сигнал с выхода антенны подается на вход приемно-регистрирующего устройства, с помощью которого по результатам измерений по определенной методике производится расчет опасных зон.

Общая схема измерения ПЭМИ приведена на рис. 1.

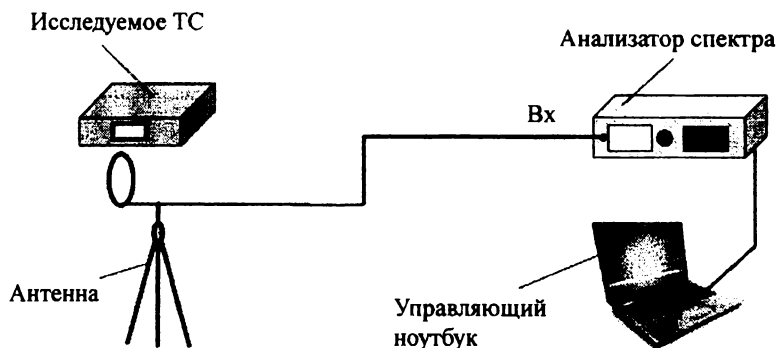


Рис. 1. Схема измерений ПЭМИ

Выявление возможных характеристик опасных сигналов производится в тестовых режимах работы технического средства. Тестовые режимы позволяют установить необходимый уровень и форму опасного сигнала и гарантированно его выделить при измерении на фоне других сигналов по известным признакам. Для выделения опасного сигнала необходимо однозначное значение трех параметров: длительности импульса, частоты следования импульсов в пакете, частоты следования пакетов.

Задача создания корректного теста решается отдельно для каждого типа СВТ после предварительного изучения вида, типа кодирования и способа передачи информации.

Стандартным тест-режимом для СИ видеоподсистемы ПЭВМ является вывод на экран видеосигнала, представляющего собой чередование черных и белых полос в режиме пиксель через пиксель. Такой сигнал представляет собой последовательность прямоугольных импульсов, у которой длительность импульса равна длительности паузы (сигнал типа «меандр»). Каждая строка раstra при этом представляет собой пакет импульсов. Число импульсов в пакете равно половине разрешения экрана по горизонтали (для режима 1024×768 это составляет 512 импульсов). Далее пауза, обусловленная обратным ходом строчной развертки, и новый пакет.

При проведении СИ клавиатуры необходимо обеспечить бесконечную подачу в кабель клавиатуры набранного символа. В обычном режиме нажатие и удержание клавиши клавиатуры приводит к переполнению буфера контроллера и нарушению режима работы. Суть тест-режима заключается в блокировании команды переполнения буфера. Постоянное чередование импульсов в кодовом пакете обеспечивает нажатие и удержание клавиши «+», которой соответствует код 55_{16} (10101010₂).

При СИ интерфейса USB осуществляется запись данных на носитель или чтение данных с носителя.

3. Создание математических моделей АМ-сигнала, ЧМ-сигнала и белого шума

Были созданы математические модели меандра, АМ-сигнала, ЧМ-сигнала и белого шума.

Моделирование производилось с использованием алгоритма быстрого (дискретного) преобразования Фурье, который заключается в следующем.

Пусть дана конечная последовательность комплексных величин $x_0, x_1, x_2, \dots, x_{N-1}$. Тогда ДПФ заключается в поиске другой последовательности $X_0, X_1, X_2, \dots, X_{N-1}$, элементы которой вычисляются по формуле

$$X_k = \sum_{n=0}^{N-1} x_n e^{-j \frac{2\pi kn}{N}}. \quad (1)$$

Теперь рассмотрим обратный случай. Пусть дана конечная последовательность комплексных величин $X_0, X_1, X_2, \dots, X_{N-1}$. Обратное ДПФ заключается в поиске другой последовательности: $x_0, x_1, x_2, \dots, x_{N-1}$, элементы которой вычисляются по формуле

$$x_n = \frac{1}{N} \sum_{k=0}^{N-1} X_k e^{j \frac{2\pi kn}{N}}. \quad (2)$$

Основным свойством этих преобразований является тот факт, что из последовательности $\{x\}$ получается (при прямом преобра-

зовании) последовательность $\{X\}$; а если потом применить к $\{X\}$ обратное преобразование, то снова получится исходная последовательность $\{x\}$.

Основная идея алгоритма вычисления БПФ состоит в двух пунктах:

- разделить сумму (1) из N слагаемых на две суммы по $N/2$ слагаемых и вычислить их по отдельности. Для вычисления каждой из подсумм их тоже нужно разделить на две и т. д.;
- повторно использовать уже вычисленные слагаемые.

Физический смысл дискретного преобразования Фурье состоит в представлении некоторого сигнала в виде суммы гармоник. Параметры каждой гармоники вычисляются прямым преобразованием, оно позволяет перейти от временного представления сигнала к спектральному (частотному) представлению; а сумма гармоник – обратным преобразованием, позволяющим перейти от спектрального представления сигнала к временному представлению.

Пакет MathLab включает набор функций, позволяющих вычислять прямое и обратное ДПФ. Эти функции могут быть использованы в приложениях путем подключения соответствующей библиотеки и вызова из нее нужной функции.

4. Воплощение

Программный интерфейс разрабатывался, исходя из требований понятности и удобства пользователю. Расположение компонентов осуществлялось по следующим принципам:

- избегание избыточности компонентов и данных в одном окне;
- объединение компонентов с однотипными функциями в отдельные блоки (например, компоненты для установления частотных границ и компоненты для установления интервала временной развертки расположены в разных блоках). Этот принцип обеспечивает не только простоту освоения программы пользователем, но и облегчает реализацию функций данных компонентов на этапе программирования;
- выбор типа расположения окон приложения остается за пользователем.

Основополагающим компонентом разрабатываемого приложения является компонент, играющий роль дисплея анализатора спектра. Данный компонент должен быть визуальным и приспособленным к отображению графической информации.

В качестве указанного компонента используется компонент Chart. Класс TChart обладает рядом свойств и методов, которые существенно упрощают реализацию виртуального анализатора спектра. К таковым можно отнести, например, автоматическое построение осей графика и подписей шкал; методы, задающие отображаемую часть графика; метод вывода координат курсора мыши; свойство Canvas, предоставляющее канву (холст) для рисования на компоненте.

5. Результат

В рамках разработки программы-симулятора ручного режима работы ПАК «Сигурд» были созданы виртуальный анализатор спектра с рабочим диапазоном частот от 9 кГц до 1 ГГц и виртуальный комплект антенн (антенны АИР 3-2, АИ 5-1 и АИ 5-0).

Разработанная программа-симулятор эмулирует сигналы ПЭМИН следующих подсистем ПЭВМ:

- видеоподсистема (монитор):
 - а) видеорежим $1280 \times 1024 \times 60$ Гц;
 - б) видеорежим $1280 \times 1024 \times 75$ Гц;
 - с) видеорежим $960 \times 600 \times 60$ Гц;
 - д) видеорежим $960 \times 600 \times 75$ Гц;
- usb-клавиатура;
- интерфейс usb v. 1.1 (режим full speed);
- интерфейс usb v. 2.0 (режим high speed).